No. 17-2

IN THE

# Supreme Court of the United States

UNITED STATES OF AMERICA,

*Petitioner,*

*v.*

MICROSOFT CORPORATION,

*Respondent.*

*On Writ of Certiorari to the United States Court of Appeals for the Second Circuit*

## BRIEF FOR *AMICUS CURIAE* EUROPEAN COMPANY LAWYERS ASSOCIATION IN SUPPORT OF RESPONDENT


Jonathan E. Marsh
EUROPEAN COMPANY LAWYERS ASSOCIATION
Rue des Sols 8
B-1000 Brussels, Belgium

Jonathan I. Blackman
*Counsel of Record*
Jared Gerber
Josh E. Anderson
Georgia V. Stasinopoulos
CLEARY GOTTLIEB STEEN & HAMILTON LLP
One Liberty Plaza
New York, New York 10006
212-225-2000
212-225-3999
jblackman@cgsh.com


January 18, 2018

*Counsel for Amicus Curiae the European Company Lawyers Association*

## TABLE OF CONTENTS


| | | Page |
|---|---|---|
| TABLE OF AUTHORITIES | | iv |
| INTEREST OF AMICUS CURIAE | | 1 |
| SUMMARY OF ARGUMENT | | 2 |
| ARGUMENT | | 3 |
| I. | THE GOVERNMENT'S POSITION RESULTS IN A DIRECT COLLISION BETWEEN SCA WARRANTS AND EUROPEAN DATA PROTECTION AND PRIVACY LAWS. | 4 |
| | A. EU Law Recognizes the Protection of Personal Data and Privacy as Fundamental Individual Rights. | 7 |
| | B. The Government's Position, If Adopted, Would Trigger Serious and Unresolvable Conflicts between SCA Warrants and European Data Protection and Privacy Rules. | 11 |

TABLE OF CONTENTS (cont'd)

Page

1. SCA Warrants May Not Supply an Adequate Legal Basis for EU Companies to Process the Personal Data Sought by the Warrant. ..... 11

2. EU Companies May Be Prohibited from Transferring Personal Data to the United States in Response to an SCA Warrant..... 14

3. Preclusion of Notice Orders Create Further Conflicts with Other Provisions of EU Law..... 17

4. Preclusion of Notice Orders Also Threaten Substantive Privilege Protections..... 19

5. EU Companies Face Significant Monetary Penalties and Potential Civil or Criminal Liability for Violating EU Privacy Laws..... 21

## TABLE OF CONTENTS (cont'd)


Page

II. THIS COURT SHOULD AFFIRM THE SECOND CIRCUIT'S DECISION IN RECOGNITION OF THE GRAVE COMITY CONSIDERATIONS AND INTERNATIONAL DISCORD THE GOVERNMENT'S POSITION CREATES..... 23

A. The Same Comity Concerns that Help Inform This Court's Extraterritoriality Jurisprudence Also Underlie *Aérospatiale*. ..... 24

B. Balancing Under *Aérospatiale* Means Affording Genuine Respect for Foreign Sovereignty and Foreign Law..... 28

CONCLUSION..... 33

## TABLE OF AUTHORITIES


| | Page(s) |
|---|---|
| **Rules and Statutes** | |
| 18 U.S.C. § 2701 *et seq.* | *passim* |
| 18 U.S.C. § 2705(b) | 17 |
| Fed. Rule Crim. Proc. 41(d) | 30 |
| **Cases** | |
| *Hudson* v. *Hermann Pfauter GmbH & Co.*, 117 F.R.D. 33 (N.D.N.Y. 1987) | 30–31 |
| *In re a Warrant to Search a Certain E–Mail Account Controlled & Maintained by Microsoft Corp.*, 829 F.3d 197 (2d Cir. 2016), reh'g denied, 855 F.3d 53 (2d Cir. 2017) | 24 |
| *In re Perrier Bottled Water Litig.*, 138 F.R.D. 348 (D. Conn. 1991) | 30 |
| *Kiobel* v. *Royal Dutch Petroleum Co.*, 569 U.S. 108 (2013) | 25 |
| *Morrison* v. *National Australia Bank Ltd.*, 561 U.S. 247 (2010) | 24–25 |

## TABLE OF AUTHORITIES (cont'd)


Page(s)

*Reinsurance Co. of Am., Inc.* v. *Administratia Asigurarilor de Stat (Admin. of State Ins.)*, 902 F.2d 1275 (7th Cir. 1990) ..... 31

*RJR Nabisco, Inc.* v. *European Community*, 579 U.S. —, 136 S. Ct. 2090 (2016) ..... 25

*Société Nationale Industrielle Aérospatiale* v. *United States District Court for the Southern District of Iowa*, 482 U.S. 522 (1987)..... *passim*

**Foreign Law**

Assemblée Nationale [National Assembly], Texte Adopté n° 69 [Text Adopted No. 69], Résolution Européenne sur le marché unique de numérique [European Resolution on the Digital Single Market] (Dec. 31, 2017), online at http://www.assembleenationale.fr/15/pdf/ta/ta0069.pdf (as visited Jan. 18, 2018) ..... 6

Charter of Fundamental Rights of the European Union, 2012 O.J. (C. 326) 391 ..... 7

## TABLE OF AUTHORITIES (cont'd)


| | Page(s) |
|---|---|
| Comm'n Decision 2000/520, 2000 O. J. (L. 215) 7 | 9 |
| Comm'n Decision 2016/1250, 2016 O. J. (L. 207) 1 | 9 |
| Criminal Justice (Mutual Assistance) Act 2008 (Act No. 7/2008) (Ir.) | 14 |
| Europ. Parl. and Coun. Directive 95/46, 1995 O. J. (L. 281) 31 | 4 |
| Europ. Parl. and Coun. Reg. 2016/679, 2016 O. J. (L. 119) 1 | *passim* |
| **Foreign Treaties** | |
| Consolidated Version of the Treaty on the Functioning of the European Union, 2012 O.J. (C. 326) 47 | 7 |
| **Foreign Cases** | |
| *Akzo Nobel Chems.* v. *Commission*, 2010 E.C.R. I–8309, I–8347 (C.J. 2010) | 19 |
| *AM & S Europe Ltd.* v. *Commission*, 1 82 E.C.R. 1575, [1982] 2 C.M.L.R. 264 (C.J. 1982) | 20 |

## TABLE OF AUTHORITIES (cont'd)


| | Page(s) |
|---|---|
| *Probst* v. *mr.nexnet GmbH*, EU:C:2012:748 (C.J. Nov. 22, 2012)..... | 15 |
| *Schrems* v. *Data Prot. Comm'r*, EU:C:2015:650, [2016] 2 C. M. L. R. 38 (C. J. Oct. 6, 2015)..... | 9 |
| **Other Authorities** | |
| Article 29 Data Protection Working Party, 00339/09/EN WP 158, Working Document 1/2009 on Pre-Trial Discovery for Cross Border Civil Litigation (adopted Feb. 11, 2009), online at http://ec.europa.eu/justice/policies/privacy/docs/wpdocs/2009/wp158_en.pdf (as visited Jan. 18, 2018)..... | 12 |
| Article 29 Data Protection Working Party, 17/EN WP 255, E.U. – U.S. Privacy Shield – First Annual Joint Review (adopted Nov. 28, 2017), online at https://iapp.org/media/pdf/resource_center/Privacy_Shield_Report-WP29pdf.pdf (as visited Jan. 18, 2018) ..... | 10 |

**TABLE OF AUTHORITIES (cont'd)**


| | Page(s) |
|---|---|
| Article 29 Data Protection Working Party, 17/EN WP260, Guidelines on Transparency Under Regulation 2016/679, online at http://ec.europa.eu/newsroom/just/document.cfm?doc_id=48850 (as visited Jan. 18, 2018) | 17 |
| Article 29 Working Party, 2093/05/EN WP 114, Working Document on a Common Interpretation of Article 26(1) of Directive 95/46/EC of 24 October 1995 (adopted Nov. 25, 2005), online at http://ec.europa.eu/justice/data-protection/article-29/documentation/opinion-recommendation/files/2005/wp114_en.pdf (as visited Jan. 18, 2018) | 15–16 |
| Executive Summary of the Opinion of the European Data Protection Supervisor on the EU-US Privacy Shield Draft Adequacy Decision, 2016 O. J. (C. 257) 8 | 10 |
| Diana Good et al., *Privilege: A World Tour* (Nov. 18, 2004), https://uk.practicallaw.thomsonreuters.com/2-103-2508?transitionType=Default&contextData=(sc.Default)&firstPage=true&bhcp=1 (as visited Jan. 18, 2018) | 20 |

## TABLE OF AUTHORITIES (cont'd)

Page(s)

David J. Kessler et al., *The Potential Impact of Article 48 of the General Data Protection Regulation on Cross Border Discovery from the United States*, 17 Sedona Conf. J. 575 (2016) ..... 29

Ministère de l'Europe et des Affaires étrangères [Ministry for Europe and Foreign Affairs], États-Unis – Union européenne - Q&R - Extrait du point de presse (4 janvier 2018) [United States – European Union - Q&A - Excerpt of Press Briefing (4 January 2018)], https://www.diplomatie.gouv.fr/fr/politique-etrangere-de-la-france/europe/actions-et-positions-de-la-france-politiques-internes-de-l-ue/justice-et-affaires-interieures/article/etats-unis-union-europeenne-q-r-extrait-du-point-de-presse-04-01-18 (as visited Jan. 18, 2018) ..... 6

Geoffrey Sant, *Court-Ordered Law Breaking: U.S. Courts Increasingly Order the Violation of Foreign Law*, 81 Brooklyn L. Rev. 181 (2015) ..... 29

## TABLE OF AUTHORITIES (cont'd)

Page(s)

Diego Zambrano, *Comity of Errors: The Rise, Fall, and Return of International Comity in Transnational Discovery*, 34 Berkeley J. Int'l L. 157 (2016) ..... 29

## INTEREST OF *AMICUS CURIAE* [1]

The European Company Lawyers Association (the "ECLA" or "*amicus*"), created in 1983, is the umbrella organization for 19 company lawyer associations in Europe. For over three decades, the ECLA has advanced common standards and best practices for in-house lawyers across the European Union and the European continent.

In-house lawyers are EU companies' first line of defense in understanding and complying with the European Union's comprehensive privacy and data protection requirements. The ECLA therefore has a strong interest in ensuring that its 42,000 constituent lawyers (who practice in 18 countries across Europe) and the companies they advise not be unnecessarily forced to choose between complying with a U.S. warrant for communications stored in Europe and violating the EU law that limits the processing and disclosure of those communications. The ECLA's constituent lawyers and their clients also have an interest in ensuring the protection of their legitimate expectations regarding the privacy and confidentiality of legal advice and privileged materials that may be included in stored

---

[1] Pursuant to this Court's Rule 37.6, *amicus curiae* hereby states that this brief was not authored in whole or in part by counsel for any party, and no such counsel or any party made a monetary contribution intended to fund the preparation or submission of this brief. No person or entity other than *amicus*, its members, or its counsel made a monetary contribution to the preparation or submission of this brief. Pursuant to this Court's Rule 37.3(a), counsel for all parties consented in writing to the filing of this brief.

communications. The question presented is therefore of critical importance to the ECLA and its constituents.

## SUMMARY OF ARGUMENT

The Government's position in this case places European companies and other companies that do business in the European Union between the irreconcilable demands of EU and U.S. law. The Government seeks to compel production of personal data stored in Ireland pursuant to a U.S. statutory provision, the Stored Communications Act, 18 U.S.C. § 2701 *et seq.* (the "SCA"), that the Government concedes was not designed to apply extraterritorially. The Government nonetheless maintains that so long as a service provider is subject to service of an SCA warrant in the United States, and disclosure of the data would be made to authorities in the United States, compliance with an SCA warrant by the service provider is required. This position creates direct conflicts with EU data protection regulations that explicitly prohibit the very transfer the Government seeks and authorize sweeping administrative penalties and private lawsuits for violations of that prohibition. Adopting the Government's view will all but assure that companies are trapped between two competing legal mandates, with no clear path for navigating that conflict.

These conflicts present clear comity concerns that cannot be lightly disregarded. Indeed, this Court's prior jurisprudence requires courts to *avoid* triggering clashes between U.S. and foreign law.

Affirming the Second Circuit's decision will advance this fundamental goal of avoiding the risk of international discord.

While the Court of Appeals' correct statutory interpretation is a sufficient ground for doing this, this Court's decision in *Société Nationale Industrielle Aérospatiale* v. *United States District Court for the Southern District of Iowa*, 482 U.S. 522 (1987) ("*Aérospatiale*"), provides an alternative basis for affirmance. The essential teaching of *Aérospatiale* is that U.S. courts, faced with cross-border disclosure questions, must engage in a careful, fact-specific balancing—weighing U.S. disclosure interests with the interests of the foreign sovereigns implicated by the disclosure request, as reflected in their laws and public policies. The blanket rule sought by the Government provides no room to weigh these competing interests. This case indeed presents the Court, 30 years after *Aérospatiale*, with an overdue opportunity to provide the lower courts with much-needed guidance on how to properly evaluate conflicts between foreign and U.S. law under the *Aérospatiale* framework. Lower courts have too often reflexively resolved such conflicts in favor of requiring U.S. disclosure, without appropriate respect for countervailing foreign sovereignty considerations.

## ARGUMENT

The Government asserts that concerns its position will lead to "international discord" are "overstated." Gov't Br. 15–16. The Government is wrong. The Government urges an interpretation of

the SCA that could effectively require any company that happens to be subject to service in the United States to make a disclosure of data in violation of EU data protection and privacy laws, without any consideration of the comity factors that *Aérospatiale* compels. The Second Circuit's ruling, on the other hand, mitigates this significant risk of international discord by acknowledging the serious comity considerations the Government seeks to bypass.

## I. THE GOVERNMENT'S POSITION RESULTS IN A DIRECT COLLISION BETWEEN SCA WARRANTS AND EUROPEAN DATA PROTECTION AND PRIVACY LAWS.

As a threshold matter, the need to engage in an *Aérospatiale* comity analysis is inescapable. The Government gives the issue the proverbial back of the hand, asserting that any conflict between EU data protection and privacy laws and SCA warrants is "speculative." Gov't Br. 50. In fact, there is nothing uncertain or "speculative" about the conflict of laws and sovereignties that the Government's position creates.

To the contrary, it is indisputable that EU law imposes comprehensive obligations for the processing of personal data housed in the European Union that are incompatible with the Government's broad interpretation of the SCA. The existing European Union Data Protection Directive of 1995, Europ. Parl. and Coun. Directive 95/46, 1995 O.J. (L. 281) 31 ("Directive"), as well as the forthcoming General Data Protection Regulation, Europ. Parl.

and Coun. Reg. 2016/679, 2016 O.J. (L. 119) 1 ("GDPR"), which becomes fully applicable in May 2018, closely regulate the processing of personal data in the context of EU business regardless of whether the processing takes place in the European Union or elsewhere. These obligations also extend to the processing of personal data carried out by companies located outside the European Union, so long as those companies offer products or services within the European Union or monitor the behavior of individuals in the European Union.[2] The GDPR, in particular, prohibits transfers of personal data to third countries outside the European Union absent a showing of compliance with data protection standards essentially equivalent to EU standards or otherwise falling within a set of specific derogations that would often not apply to SCA warrants, and additionally imposes stringent transparency requirements that could directly conflict with the requirements of SCA warrants. The GDPR also imposes severe penalties for noncompliance with these rules.

Other *amici* discuss at length the structure and requirements of EU data protection and privacy law, and how "[t]here is . . . no doubt that the European Union is actively regulating the issues at this case's heart." European Comm'n Amicus Br. 5. A number

---

[2] Consistent with the approach taken by the European Commission (European Comm'n Amicus Br. 2–3, n. 5), this brief focuses on the GDPR rules most likely to be applicable to an SCA warrant. In substance, the provisions of the GDPR and the Directive on the transfer of personal data to a non-EU state are largely similar. *See* European Comm'n Amicus Br. 2–3, n. 5.

of those *amici* are foreign governments who have expressed their reservations about the possible implications of the Government's approach.[3] In particular, both the French National Assembly and the French Government have issued public statements regarding this litigation, in which they express concern about the significant risk of conflict between U.S. and European law and reiterate France's preference for law enforcement cooperation through international conventions.[4]

From the standpoint of the regulated companies and their in-house lawyers represented by the ECLA, the problem can be stated in much starker terms: the Government's expansive reading of its authority under the SCA, if adopted, would all but

---

[3] *See, e.g.*, United Kingdom Amicus Br. (in support of neither party); New Zealand Privacy Commissioner Amicus Br. (in support of neither party); Ireland Amicus Br. (in support of neither party).

[4] *See* Ministère de l'Europe et des Affaires étrangères [Ministry for Europe and Foreign Affairs], États-Unis – Union européenne - Q&R - Extrait du point de presse (4 janvier 2018) [United States – European Union - Q&A - Excerpt of Press Briefing (4 January 2018)], https://www.diplomatie.gouv.fr/fr/politique-etrangere-de-la-france/europe/actions-et-positions-de-la-france-politiques-internes-de-l-ue/justice-et-affaires-interieures/article/etats-unis-union-europeenne-q-r-extrait-du-point-de-presse-04-01-18 (as visited Jan. 18, 2018); *see also* Assemblée Nationale [National Assembly], Texte Adopté n° 69 [Text Adopted No. 69], Résolution Européenne sur le marché unique de numérique [European Resolution on the Digital Single Market], at 4, 6 (Dec. 31, 2017), online at http://www.assemblee-nationale.fr/15/pdf/ta/ta0069.pdf (as visited Jan. 18, 2018).

ensure real, unavoidable and serious conflicts between EU data protection requirements and SCA warrant compliance. Adopting the Government's position would trap such companies between two competing legal regimes, and expose them to considerable financial and legal risk in complying with SCA warrants.

### A. EU Law Recognizes the Protection of Personal Data and Privacy as Fundamental Individual Rights.

There are significant differences between the privacy protections recognized under U.S. and EU law. In the European Union, unlike in the United States, both the right to privacy as well as the right to the protection of personal data are recognized as fundamental individual rights. Article 8 of the European Union's Charter of Fundamental Rights provides: "Everyone has the right to the protection of personal data . . . . Such data must be processed fairly for specified purposes and on the basis of the consent of the person concerned or some other legitimate basis laid down by law." 2012 O.J. (C. 326) 391. The Treaty on the Functioning of the European Union, which provides the modern European Union's constitutional basis, similarly recognizes the protection of personal data as a fundamental right for EU residents, and requires the creation of rules to protect residents' personal data. *See* Consolidated Version of the Treaty on the Functioning of the European Union, Art. 16, 2012 O.J. (C. 326) 47.

The principle that the protection of personal data and privacy are fundamental rights animates the comprehensive framework of EU regulations with which companies must comply when storing, processing and transferring personal data. This regime not only protects individuals from unauthorized use of their data, but also establishes certain affirmative rights and guarantees, strengthened in the GDPR. *See, e.g.*, GDPR, Arts. 12–14 (transparency and right to information regarding the processing of personal data), 15 (right of access to personal data that is processed), 16 (right to correction of personal data), 17 (right to obtain erasure of processed personal data, i.e., the 'right to be forgotten'), 21 (right to object to the processing and transfer of personal data), 82 (private right of action against companies that mishandle data). Under the GDPR, these rights are further guaranteed by the availability of significant penalties imposed on offending companies. *See* GDPR, Art. 83.

These regulations also reflect a clear desire to ensure that the rights and protections of EU law continue to apply even where data is transferred outside the European Union, especially when data is transferred to third countries like the United States with less robust personal data guarantees.[5] Where the corresponding protections fall below EU standards, transfers of personal data to those third

---

[5] *See, e.g.*, GDPR, Art. 45(2) (identifying specific factors the European Commission should take into account in rendering decisions about the adequacy of other countries' personal data protection).

countries are presumptively prohibited. *See* GDPR, Arts. 44–46. Unlike certain other third countries that the European Union has recognized as providing an adequate level of personal data protection, past adequacy decisions issued with respect to the United States have instead been limited to the commercial context and conditioned on participation by companies in a self-certification program.[6] These self-certification schemes aim to ensure that companies transferring personal data to the United States have implemented protections and guarantees essentially equal to the EU data protection and privacy requirements. However, the European Commission has, to date, been unable to issue an unconditional adequacy decision with respect to the U.S. legal framework that would permit free transfers of personal data to the United States, in effect finding that absent the steps required by the self-certification program, the background privacy protections in the United States

---

[6] In 2000, the European Union issued an initial adequacy decision for the United States under the U.S.-EU Safe Harbor Framework, which permitted organizations to self-certify that they provide an adequate level of protection for personal data transferred from the European Union. Comm'n Decision 2000/520, 2000 O.J. (L. 215) 7. However, this arrangement was invalidated by the Court of Justice of the European Union in October 2015. *Schrems* v. *Data Prot. Comm'r* ("*Schrems I*"), EU:C:2015:650, [2016] 2 C.M.L.R. 38 (C.J. Oct. 6, 2015). In February 2016, following extensive negotiations with the United States, the European Commission issued the new EU-U.S. Privacy Shield Framework, which permits U.S. organizations to join and demonstrate compliance with that framework in order to be permitted to facilitate limited cross-border data transfers. *See* Comm'n Decision 2016/1250, 2016 O.J. (L. 207) 1.

are insufficient to meet EU requirements and standards.[7]

The European Union's commitment to the protection of personal data and privacy has been strengthened by the adoption of the GDPR in 2016. The GDPR repeals and replaces the Directive and significantly strengthens the restrictions on the transfer of personal data to third countries, as explained more fully below. Importantly, the GDPR will in many cases apply to companies processing personal data in the European Union or of EU residents regardless of the company's location. *See* GDPR, Art. 3 *et seq.* Accordingly, companies like Microsoft that offer services to EU residents, and in that capacity store or process personal data, are subject to the substantive requirements of the GDPR.

---

[7] In May 2016, the European Data Protection Supervisor issued the following opinion with respect to the Privacy Shield: "The draft Privacy Shield may be a step in the right direction *but as currently formulated it does not adequately include . . . all appropriate safeguards to protect the EU rights of the individual to privacy and data protection also with regard to judicial redress.*" Executive Summary of the Opinion of the European Data Protection Supervisor on the EU-US Privacy Shield Draft Adequacy Decision, 2016 O.J. (C. 257) 8 (emphasis added); *see also* Article 29 Data Protection Working Party, 17/EN WP 255, E.U. – U.S. Privacy Shield – First Annual Joint Review (adopted Nov. 28, 2017) (noting similar concerns about scope of Privacy Shield), online at https://iapp.org/media/pdf/resource_center/Privacy_Shield_Report-WP29pdf.pdf (as visited Jan. 18, 2018).

### B. The Government's Position, If Adopted, Would Trigger Serious and Unresolvable Conflicts between SCA Warrants and European Data Protection and Privacy Rules.

To the extent the Government's position prevails, companies doing business in the European Union risk being forced to choose between compliance with SCA warrants and at least three core aspects of EU law, which are enforceable both by data protection authorities in the European Union and through private rights of action: (1) restrictions on the "processing" of personal data; (2) restrictions on transfers of personal data to the United States; and (3) requirements to provide notice to the individual whose data is sought by the warrant, as well as to data protection authorities in the EU member states.

#### 1. SCA Warrants May Not Supply an Adequate Legal Basis for EU Companies to Process the Personal Data Sought by the Warrant.

Under Article 6(1) of the GDPR, a company must have a legal basis for "processing" personal data. Processing is a broad concept, which encompasses certain steps that would be required to respond to an SCA warrant, including retrieving data stored on a server in the European Union, transferring that data to the United States for disclosure and actually disclosing it to authorities in the United States. *See* GDPR, Art. 4(2). An SCA warrant alone will often

not supply a sufficient legal basis for data processing under European law.

Indeed, the limited legal bases set out in the GDPR to legitimize the processing of personal data will plainly *not* be available in the context of an SCA warrant. First, consent of the individuals to whom the data relates (i.e., the data subjects) is not practicable as a legal basis for providing data under an SCA warrant. While consent is a ground for processing under Article 6(1)(a) of the GDPR, the Article 29 Working Party, an independent advisory body established under the Directive, has noted that in most cases, consent is unlikely to provide a sufficient basis for transfer of personal data to a foreign jurisdiction because valid consent requires that the data subject have a real opportunity to withhold or subsequently withdraw her consent at any time. *See* GDPR, Art. 7(3).[8] Moreover, consent is also unlikely to be satisfied in a law enforcement context that involves issuance of warrants without notice to the data subject.

Likewise, while compliance with an SCA warrant may be found to be necessary for the purposes of a legitimate interest pursued by the data controller or a third party, this basis would only be applicable where this interest is not "overridden by the interests or fundamental rights and freedoms of the data subject." GDPR, Art. 6(1)(f). In the law

---

[8] *See also* Article 29 Data Protection Working Party, 00339/09/EN WP 158, Working Document 1/2009 on Pre-Trial Discovery for Cross Border Civil Litigation 8–9 (adopted Feb. 11, 2009), online at http://ec.europa.eu/justice/policies/privacy/docs/wpdocs/2009/wp158_en.pdf (as visited Jan. 18, 2018).

enforcement context, satisfying such a balancing test could be practically impossible, given the potential risks and consequences of disclosure for data subjects. In any event, this legal basis would also require the company to which the request has been made to have the information necessary to assess and balance various competing considerations, which it often will not have in the context of an investigation by law enforcement.[9]

An additional possible ground recognized under EU law for processing data is where doing so is "necessary for compliance with a legal obligation to which the controller is subject." GDPR, Art. 6(1)(c). Critically, however, any such legal obligation must arise out of EU law or the national law of an EU member state. *See* GDPR, Art. 6(3). Accordingly, an obligation under U.S. law alone would *not* be a valid ground to process or transfer data in the European Union.

The final possibly relevant ground for processing data recognized by EU law is where compliance would be "necessary for the performance of a task carried out in the public interest." GDPR, Art. 6(1)(e). However, this basis is inapplicable here; as with other provisions, only EU law or the law of a

---

[9] As discussed below, to the extent a company relies on the "legitimate interests" basis to transfer personal data to a third country, the GDPR gives data subjects the right to object to the processing of their personal data, inviting additional practical conflicts between SCA warrants and the GDPR. *See* GDPR, Art. 21(1).

member state can supply the required legal ground. *See* GDPR, Art. 6(3).

2. EU Companies May Be Prohibited from Transferring Personal Data to the United States in Response to an SCA Warrant.

Even if there were a legal basis for processing the personal data sought by an SCA warrant, the GDPR further restricts the transfer of personal data to third countries that fail to meet certain personal data requirements. In this regard, the GDPR has a clear preference for making any transfers pursuant in response to a "judgment of a court or tribunal [or a] decision of an administrative authority of a third country requiring a controller or processor to transfer or disclose personal data" *only* under the auspices of international agreements, such as mutual legal assistance treaties ("MLATs"). GDPR, Art. 48; European Comm'n Amicus Br. 14 (quoting same). The specific intention of Article 48, as reflected in the recital explaining this Article, was to address "[t]he extraterritorial application of those laws, regulations and other legal acts [that] may impede the attainment of the protection of natural persons ensured in the Union by this Regulation." GDPR, Art. 48, Recital 115. The United States has executed MLATs with a number of EU member states, including Ireland.[10] But the Government's position, if adopted, would have the effect of circumventing both the intent of EU law under

---

[10] Criminal Justice (Mutual Assistance) Act 2008 (Act No. 7/2008) (Ir.).

Article 48 and the international agreements the United States has made. If the Government refuses to avail itself of the MLAT process, where such a process exists, companies cannot transfer personal data to the United States unless they satisfy other requirements of the GDPR.

In sum, provided that no international agreement or other contractual tools are applicable, the transfer of personal data to the United States in response to an SCA warrant is presumptively prohibited by the GDPR. *See* GDPR, Arts. 44–46. While there are exceptions to this presumptive bar, called "derogations," those exceptions are narrowly construed, *see* European Comm'n Amicus Br. 16; *Probst* v. *mr.nexnet GmbH*, EU:C:2012:748, ¶ 23 (C.J. Nov. 22, 2012) (enumerated exceptions to protections of the confidentiality of communications should be interpreted strictly), and in many circumstances, will not apply.

First, while there is a public interest derogation that is applicable for "important reasons of public interest," GDPR, Art. 49(1)(d), this derogation would not be applicable to many SCA warrant situations, because the derogation *only* applies where the interest is founded on EU law or the law of an EU member state, *see* GDPR, Art. 49(4), and cannot be based on a "unilateral decision by a third country."[11]

---

[11] Article 29 Working Party, 2093/05/EN WP 114, Working Document on a Common Interpretation of Article 26(1) of Directive 95/46/EC of 24 October 1995, at 14–15 (adopted Nov. 25, 2005), online at http://ec.europa.eu/justice/data-protection/

A second potentially applicable derogation permits transfers to third countries where there are "compelling legitimate interests" that override "the interests or rights and freedoms of the data subject." GDPR, Art. 49(1). However, this derogation carries with it a number of additional restrictions and requirements, including that the derogation is applicable only where "the transfer is not repetitive" and "concerns only a limited number of data subjects." *Ibid.* Moreover, before a data service provider can rely on this derogation to transfer personal data, it must "asses[s] all the circumstances surrounding the data transfer," GDPR, Art. 49(1), which would require information that a recipient of an SCA warrant will often lack, and which the Government may not be willing to provide. Similarly, a company cannot rely on the derogation unless it forms the "assessment [that] suitable safeguards with regard to the protection of personal data" will be provided by the transferee. *Ibid.* But a service provider served with an SCA warrant has little meaningful ability to negotiate how the Government will hold and safeguard any data the company discloses. Finally, this derogation also requires that the company inform the competent data protection authority and the data subject of the transfer. Disclosure of data could then be subject to potential legal challenges before EU data protection authorities, which could result in companies being forced to choose whether to comply

---

article-29/documentation/opinion-recommendation/files/2005/wp114_en.pdf (as visited Jan. 18, 2018).

with the SCA warrant or with a contrary order of an EU authority.

3. Preclusion of Notice Orders Create Further Conflicts with Other Provisions of EU Law.

In connection with SCA warrants, the Government is authorized to seek "preclusion of notice" orders, which prohibit providers from notifying "any other person of the existence of the warrant." 18 U.S.C. § 2705(b). Obtaining such an order in the case of an SCA warrant directed at personal data covered by the GDPR would produce yet another direct conflict with EU transparency requirements. The GDPR's transparency requirement concerning the processing of personal data, Art. 5(1)(a), is "an expression of the principle of fairness in relation to the processing of personal data expressed in Article 8 of the Charter of Fundamental Rights of the European Union."[12]

The GDPR gives the data subject the right to be notified of the processing of their personal data, including a transfer to a third country, to ensure the ability of the data subject to exercise their rights. *See* GDPR, Art. 13 *et seq.*; *see also* GDPR, Art. 49(1) (to the extent transfer is based on the "compelling legitimate interests" derogation, the data subject must also be informed of both the transfer and the interests pursued). Under specified circumstances,

---

[12] Article 29 Data Protection Working Party, 17/EN WP260, Guidelines on Transparency Under Regulation 2016/679, ¶ 2, online at http://ec.europa.eu/newsroom/just/document.cfm?doc_id=48850 (as visited Jan. 18, 2018).

a company is also obligated to notify the data protection authorities of the transfer. *See* GDPR, Art. 49(1) (the data controller "shall inform the supervisory authority of the transfer" to the extent it relies on the "compelling legitimate interests" derogation). Moreover, under Article 15(1) of the GDPR, the data subject has a "right of access" that allows him or her, at any time, to affirmatively request confirmation of whether his or her personal data has been, or is being, processed. The Government's position would permit it to impose a "gag order" on the recipient of an SCA warrant that is in direct conflict with these obligations and rights.

The transparency obligations under the GDPR support the data subject's related "right to object" to the processing of his or her data. *See* GDPR, Art. 21 *et seq.*; *see also* GDPR, Art. 5(1)(a) (establishing that data be processed "lawfully, fairly and in a transparent manner in relation to the data subject"). Specifically, an individual can object to a data controller's finding that "legitimate grounds for the processing . . . override the interests, rights and freedoms of the data subject." GDPR, Art. 21(1). In the event of such a challenge, the data controller must suspend processing until the data subject's challenge can be adjudicated. *See ibid.*; GDPR, Art. 18(1)(d). Accordingly, a preclusion of notice order would effectively prevent data subjects from availing themselves of the safeguards provided by EU law to obtain recourse from EU authorities against inappropriate data processing, including transfers.

Furthermore, even to the extent no such order is obtained by the Government from the SCA warrant-

issuing U.S. court, companies may find themselves in circumstances in which the enforceability of an SCA warrant is subject to challenge by the data subject under EU law. Such a challenge would, at the very least, impact the timeline on which a company found itself able to comply with an SCA warrant, and could conceivably result in a directive prohibiting compliance with the SCA warrant altogether, again exposing the company to a conflict between compliance with the SCA warrant and compliance with EU law.

4. Preclusion of Notice Orders Also Threaten Substantive Privilege Protections.

EU law also safeguards the protection of legal privilege. *Amicus'* constituent lawyers are particularly concerned that the lack of notice afforded to the subject of an SCA warrant will deprive them and their clients of the right to take the necessary steps to assert or defend any privileges that attach to the data sought by the warrant.

It is a general principle of EU law that legal privileges must be protected. *See Akzo Nobel Chems.* v. *Commission*, 2010 E.C.R. I–8309, I–8347 (C.J. 2010) (noting that legal professional privileges "not only serv[e] to ensure the rights of defence of the client but [are] also an expression of the lawyer's status as an independent legal adviser and 'collaborat[or] in the administration of justice' who gives legal advice 'to all those who need it'" (third alteration in original)). While privilege law varies

across the European Union, most member states have laws restricting access to privileged data, and providing individuals with a forum for challenging (or defending) privilege designations. *See AM & S Europe Ltd.* v. *Commission*, 1982 E.C.R. 1575, [1982] 2 C.M.L.R. 264 (C.J. 1982) (recognizing that privilege is common to all member states in EU law, even if the scope and level of protection vary by member state).

In Belgium, for example, national law recognizes procedural protections for privilege that would be incompatible with the disclosure process mandated by SCA warrants. Under the Belgian Judicial Code, correspondence between Belgian lawyers is "confidential in principle" and cannot be used as evidence, and any potential conflict or dispute as to a privilege claim must be resolved by the head of the Belgian bar association.[13]

Accordingly, the cross-border production of potentially-privileged materials threatens to compromise the sanctity of the advice that *amicus*' constituent lawyers give to their clients, without providing them or their clients with any mechanism to take the steps necessary to secure the protections granted by EU law.

As a consequence, if the Government's position prevails, European companies and their attorneys would face a number of practical challenges in

---

[13] *See* Diana Good et al., *Privilege: A World Tour* (Nov. 18, 2004), https://uk.practicallaw.thomsonreuters.com/2-103-2508?transitionType=Default&contextData=(sc.Default)&firstPage=true&bhcp=1 (as visited Jan. 18, 2018).

protecting the confidentiality of their communications. For example, they would have a strong incentive to conduct all communications through service providers that are not subject to the jurisdiction of U.S. courts. The result would be increased complexity and costs for European companies and their counsel and reduced competition in the market for online services.[14]

5. EU Companies Face Significant Monetary Penalties and Potential Civil or Criminal Liability for Violating EU Privacy Laws.

The Government's contention that "no . . . consequences have ensued," Gov't Br. 46, from the historical extraterritorial enforcement of SCA warrants appears to be based on the premise that companies should be required to violate EU law so long as they face limited financial or enforcement risk in doing so. While *amicus* rejects this proposition, and is committed to ensuring that European companies abide by all applicable laws, the Government's position also fails to take account of the more robust enforcement environment that the GDPR introduces, as well as the risk of reputational harm companies may face after being accused of breaching EU data protection laws.

Under the GDPR, companies that fail to comply with EU data protection and privacy regulations face serious administrative fines, civil penalties

---

[14] Notably, the Article 49 derogations discussed in Section I(A)(2), *supra*, provide no basis for invading legal privilege.

and—in some member states—criminal liability. For example, if a company fails to adhere to the core requirements for processing or disclosure of personal data set forth under Articles 5 and 6 of the GDPR, or transfers personal data to a foreign country or organization without providing an adequate legal basis pursuant to the GDPR as set forth in Articles 44 through 49, it may be subject to a fine from data protection authorities of the greater of €20 million or four percent of global annual turnover in the prior year. *See* GDPR, Art. 83(5); *see also* GDPR, Art. 58 (data protection authorities have the authority to investigate breaches of the GDPR). In addition to these administrative fines, the GDPR also establishes a private cause of action for individuals who suffer an injury as a result of a breach of the GDPR, and permits member states to impose other "effective, proportionate and dissuasive" penalties. GDPR, Arts. 82, 83(9). Some member states indeed impose severe criminal sanctions, such as imprisonment, for violation of data protection rules.[15] Therefore, if the Government's position were to prevail, companies would encounter a number of potentially disruptive legal, financial and reputational risks.

---

[15] For example, breaches of the French Data Protection Act are punishable by up to five years' imprisonment or a fine pursuant to Article 226-16 *et seq.* of the French Criminal Code. Similar criminal law provisions are incorporated in the prevailing Data Protection Acts of a number of member states, including Denmark, Belgium and the United Kingdom. *See* Good et al., *supra* n. 13 (providing summary of relevant national legislation).

## II. THIS COURT SHOULD AFFIRM THE SECOND CIRCUIT'S DECISION IN RECOGNITION OF THE GRAVE COMITY CONSIDERATIONS AND INTERNATIONAL DISCORD THE GOVERNMENT'S POSITION CREATES.

Notwithstanding these conflicts with EU law that the Government's absolutist position creates—and, indeed, without even meaningfully addressing them—the Government asserts that any service provider subject to service of an SCA warrant is required to produce any data of which it has possession, custody or control, regardless of the resulting violation of foreign law. But this is precisely the situation that the nuanced determination required by *Aérospatiale* was crafted to address. *Aérospatiale* requires lower courts to take account of foreign law when dealing with cross-border disclosure issues in an ever more interconnected world in which sovereigns, if for no other reason than self-interest, must pay attention to the laws and legal policies of other sovereigns. That is why comity is important, and why the Government's approach that sweeps comity issues under the rug should be rejected. A proper application of *Aérospatiale* should lead to affirmance of the Second Circuit regardless of how the issue of the "focus" of the SCA is resolved, and at a minimum, if the Court does not affirm, should lead to a remand to apply the *Aérospatiale* factors.

Enforcement of an SCA warrant under these facts is plainly an extraterritorial application of the

SCA. [16] As the lower court correctly noted, the text of the SCA contains "powerful clues . . . which lead [it] to conclude that an SCA warrant may reach only data stored within United States boundaries." *In re a Warrant to Search a Certain E–Mail Account Controlled & Maintained by Microsoft Corp.*, 829 F.3d 197, 221 (2d Cir. 2016), reh'g denied, 855 F.3d 53 (2d Cir. 2017). Those textual clues are even more salient in light of the Government's efforts to invade the legal domain of another sovereign in order to compel the production of information stored in another country. The Government's arguments to the contrary are especially unpersuasive in light of this Court's holding in *Aérospatiale* recognizing that comity concerns are essential for resolving "cases [which] touc[h] the laws and interests of other sovereign states." 482 U.S. at 543, n. 27.

### A. The Same Comity Concerns that Help Inform This Court's Extraterritoriality Jurisprudence Also Underlie *Aérospatiale*.

Conflict avoidance, to which the Government gives short shrift, is a key part of this Court's extraterritoriality jurisprudence. The "longstanding

---

[16] *Amicus* agrees with Microsoft's argument that the Government seeks to apply the SCA in an impermissibly extraterritorial manner. *See* Microsoft Br. 20–37. Even to the extent the Court finds that the warrant at issue here does not constitute an extraterritorial application of the SCA, however, *Aérospatiale* requires a court to consider an additional set of critical considerations before it orders the cross-border disclosure of information, and here those factors provide an additional basis for affirming the decision below.

principle of American law" that presumes against the extraterritorial reach of statutes absent contrary congressional intent, *Morrison* v. *National Australia Bank Ltd.*, 561 U.S. 247, 255 (2010) (quoting *EEOC* v. *Arabian Am. Oil Co.* ("*Aramco*"), 499 U.S. 244, 248 (1991)), "serves to protect against unintended clashes between our laws and those of other nations which could result in international discord," *Kiobel* v. *Royal Dutch Petroleum Co.*, 569 U.S. 108, 115 (2013) (quoting *Aramco*, *supra*); *RJR Nabisco, Inc.* v. *European Community*, 579 U.S. —, —, 136 S. Ct. 2090, 2100 (2016) (the presumption against extraterritoriality "[m]ost notably . . . serves to avoid the international discord that can result when U.S. law is applied to conduct in foreign countries.")

Thus, in *Morrison*, when the Court rejected extraterritorial application of the Securities Exchange Act of 1934, it noted that the "probability of incompatibility with the applicable laws of other countries is so obvious that if Congress intended such foreign application it would have addressed the subject of conflicts with foreign laws and procedures." 561 U.S. at 269 (internal quotation marks omitted). Justice Breyer, in his concurrence in *Kiobel*, similarly noted that the adjudication of claims under the Alien Tort Statute must "also be consistent with those notions of comity that lead each nation to respect the sovereign rights of other nations by limiting the reach of its own laws and their enforcement." 569 U.S. at 128–29.

The same comity concern is of course at the heart of *Aérospatiale*, which, unlike the Court's statutory extraterritoriality cases, actually deals with the

issue of cross-border disclosure raised by the present case. In *Aérospatiale*, this Court refused to adopt a blanket rule requiring or disallowing resort to the Hague Evidence Convention for the purpose of civil discovery from overseas litigants, instead requiring a "particularized analysis of the respective interests of the foreign nation and the requesting nation," 482 U.S. at 543–44, with "scrutiny in each case of the particular facts, sovereign interests, and likelihood that resort to [proposed] procedures will prove effective," *id.* at 544.

The Court, following the Restatement (Third) of Foreign Relations Law of the United States, identified the following factors that should "guide a comity analysis":

> (1) the importance to the ... litigation of the documents or other information requested;
> (2) the degree of specificity of the request;
> (3) whether the information originated in the United States;
> (4) the availability of alternative means of securing the information; and
> (5) the extent to which noncompliance with the request would undermine important interests of the United States, or compliance with the request would undermine important interests of the state where the information is located.

*Id.* at 544, n. 28 (internal quotation marks omitted).

In the present case, where there has been no showing by the Government that the information sought by Microsoft originated in the United States, where the U.S.-Ireland MLAT furnishes a clear alternative means of securing the information sought by the SCA warrant,[17] and where there is a clear conflict with foreign law with significant penalties attached to non-compliance with it, the balance of these factors would tilt toward granting comity to the European Union's and Ireland's interest in enforcing their data protection laws, and denying the Government's demand for information stored in Ireland when disclosure would violate these laws.

The Government's position simply ignores *Aérospatiale*'s particularized inquiry. Instead, the Government advocates for the blanket rule that SCA warrants reach foreign stored data, so long as that data is ultimately disclosed in the United States, regardless of the countervailing foreign interests that *Aérospatiale* recognizes. Remarkably, the Government argues that the primary relevance of *Aérospatiale* is limited to the circumstances of assessing *contempt* sanctions following a party's *failure* to produce requested information. *See* Gov't Br. 51–52. However, the purpose of the comity doctrine is not just to mitigate the consequences of complying with foreign law when in conflict with

---

[17] Indeed, the Irish Government has filed an *amicus* brief which expresses that it is ready to work with the Government to provide the requested data, and that it considers "that the procedures provided for in the MLAT represent the most appropriate means to address requests such as those which are the object of the warrant in question." Ireland Amicus Br. 2.

U.S. law; it is to harmonize apparently competing laws such that the subject can comply with both laws and offense is not caused to either sovereign. Thus, companies should not be forced to make the decision to violate a U.S. court order so as to comply with EU privacy laws, with all the reputational and financial consequences entailed, on a gambler's hope that a U.S. court may later "go easy" on it at the sanctions stage. Comity requires that a respectful balance be found between foreign law and U.S. law.

To be sure, it may not be invariably the case that any foreign law will outweigh the need to enforce an SCA warrant, or other disclosure procedure; that is the reason why *Aérospatiale* demands a "particularized" inquiry. But the Government's approach, which would ignore this inquiry altogether, or relegate it to the contempt stage, flies in the face of what comity and *Aérospatiale* require. On the record in the present case, the *Aérospatiale* inquiry should lead to affirmance of the Court of Appeals, in light of the location of the information sought, the clear conflict with EU law and the alternative means of obtaining the information in conformity with EU law.

### B. Balancing Under *Aérospatiale* Means Affording Genuine Respect for Foreign Sovereignty and Foreign Law.

As other *amici* and commentators have noted, in the three decades since *Aérospatiale*, district courts have applied the balancing test in ways that often reflexively find in favor of disclosure. *See, e.g.*, E-Discovery Institute et al. Amicus Br. 17–21

(collecting cases and noting "comity's value in principle outweighs its value in practice"). While dozens of courts have considered the issues presented by *Aérospatiale* since its publication, only a small fraction of them have excused a foreign entity from a cross-border discovery or production demand in the face of a foreign law conflict. *See* Diego Zambrano, *Comity of Errors: The Rise, Fall, and Return of International Comity in Transnational Discovery*, 34 Berkeley J. Int'l L. 157, 178, n. 126 (2016) (collecting cases).

Courts have in particular given outsized weight to the U.S.-interests aspect of the fifth *Aérospatiale* factor (which is almost invariably seen as militating in favor of disclosure), while at the same time giving little regard to the importance of the interests, under the same factor, of the foreign state where the information is located. *See, e.g.*, David J. Kessler et al., *The Potential Impact of Article 48 of the General Data Protection Regulation on Cross Border Discovery from the United States*, 17 Sedona Conf. J. 575, 600–603 (2016) (collecting cases) ("Applying the fifth factor, most courts have concluded that discovery should proceed under the Federal Rules as opposed to the Hague Convention"). Many courts have in practice considered an assumed U.S. interest in wide-reaching discovery, even in cases of purely private civil litigation, to function as a trump card over all competing foreign concerns. *See* Geoffrey Sant, *Court-Ordered Law Breaking: U.S. Courts Increasingly Order the Violation of Foreign Law*, 81 Brooklyn L. Rev. 181, 219–221 (2015) (collecting cases). This approach often makes a nullity of the other four *Aérospatiale* factors and

improperly discounts the weighing of competing foreign law interests, such as the EU data protection and privacy law interests at stake here. It also downgrades the importance of another U.S. interest—comity—the "do unto others" principle that is often at least as much a U.S. interest as assuming that a U.S. choice of broader discovery is always the preeminent interest.

This case presents this Court with an opportunity to provide lower courts with further guidance concerning the proper application and weighing of the *Aérospatiale* factors. While the issuance of such a warrant presupposes a determination that there is probable cause to believe that the records to be disclosed contain evidence of a crime, Fed. Rule Crim. Proc. 41(d), at least presumptively satisfying the first two factors, the fifth factor, applied in a way consistent with *Aérospatiale*'s comity underpinnings, should in appropriate cases result in a finding *against* disclosure when a U.S. procedure violates a foreign state's laws. As some lower courts have properly recognized, unambiguous expressions by foreign states of a preference for alternative discovery procedures should weigh heavily against forced disclosure. *See In re Perrier Bottled Water Litig.*, 138 F.R.D. 348, 355 (D. Conn. 1991) (noting that France had been "emphatic" about permitting foreign discovery only within the framework of the Hague Evidence Convention, including by amending its laws to prescribe alternative procedures, which constituted "an expression of France's sovereign interests" and weighed "heavily in favor of the use of those procedures"); *see also Hudson* v. *Hermann*

*Pfauter GmbH & Co.*, 117 F.R.D. 33, 38 (N.D.N.Y. 1987) (ordering discovery be taken through the Hague Evidence Convention, noting, among other reasons a concern that private discovery in West Germany implicated "constitutional principle of proportionality, pursuant to which a judge must protect personal privacy, commercial property, and business secrets" (quoting *Aérospatiale*, 482 U.S., at 558)); *Reinsurance Co. of Am., Inc.* v. *Administratia Asigurarilor de Stat (Admin. of State Ins.)*, 902 F.2d 1275, 1280 (7th Cir. 1990) (Romania's interest outweighed U.S. interest where Romanian law categorized requested information as a state secret, and imposed sanctions for its disclosure).

Application of *Aérospatiale*'s fifth factor to preclude issuance of an SCA warrant in appropriate circumstances would accord proper respect to the European Union's expressed intention under the GDPR to protect individuals' "right to the protection of personal data," GDPR, Art. 1(2), and to the fact that data protection is considered a fundamental right in the European Union, protected under human rights treaties and the European Union's constitutional documents. *See* Section I(A), *supra*; GDPR, Recital 1. It would also permit courts to recognize in appropriate cases the preference under Article 48 of the GDPR for transferring personal data under the framework of international agreements such as MLATs, and that companies that comply with an SCA warrant might face the risk of administrative penalties and private lawsuits for violating provisions of the GDPR. *See* GDPR, Arts. 82–84. The availability of alternative methods of obtaining the information like—as in this case—

MLATs would similarly weigh against disclosure under *Aérospatiale*'s fourth factor.

At the same time, the application of *Aérospatiale* would not preclude the Government from using an SCA warrant in those circumstances where the data was not otherwise available to the Government and where no significant foreign interests were implicated. The Government's demand for blanket disclosure regardless of the location of the data and the consequent applicability of foreign data protection rules is incompatible with the considered analysis mandated by *Aérospatiale*. That analysis requires the competing interests of foreign jurisdictions to be meaningfully weighed in each case in order to achieve a result that satisfies the interests of both the United States and the relevant foreign jurisdictions in preserving comity and avoiding international discord.

## CONCLUSION

For the foregoing reasons, the decision below should be affirmed.

Respectfully submitted,

Jonathan E. Marsh
EUROPEAN COMPANY LAWYERS ASSOCIATION
Rue des Sols 8
B-1000 Brussels,
Belgium

Jonathan I. Blackman
*Counsel of Record*
Jared Gerber
Josh E. Anderson
Georgia V. Stasinopoulos
CLEARY GOTTLIEB STEEN & HAMILTON LLP
One Liberty Plaza
New York, New York
10006
212-225-2000
212-225-3999
jblackman@cgsh.com

*Counsel for Amicus Curiae the European Company Lawyers Association*

January 18, 2018